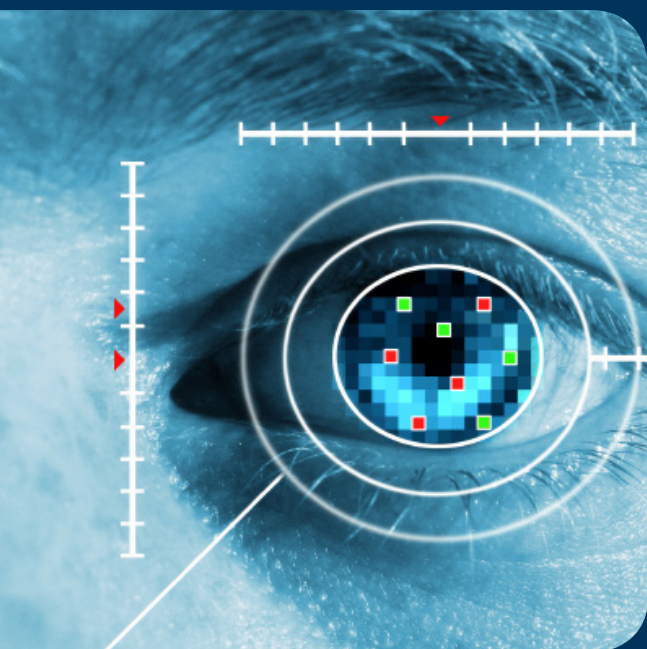


SEC150

Comprehensive Security Briefing



Exceptional service in the national interest



**Sandia
National
Laboratories**

Sandia National Laboratories

SEC150

Comprehensive Security Briefing

CONTENTS

Overview and Background	3
We Are a National Security Laboratory	3
Where Do You Fit In?	3
Security Threats Are REAL... ..	3
Some Sobering Facts	4
Use Operations Security (OPSEC)	4
You Already Understand and Practice Security	4
Information Must Be Protected.....	5
Need to Know.....	5
Understanding the Clearance Process	6
Personnel Security Program Purpose.....	6
Security Clearances	6
Adjudication	6
Due Process	7
About That Badge	8
SNL Local Site-specific Only (LSSO) Badges	8
Homeland Security Presidential Directive 12 (HSPD-12)	8
Standard Form (SF) 312, <i>Classified Information</i>	
<i>Nondisclosure Agreement</i>	9
Badge Responsibilities	9
Maintaining Your Clearance	10
Report Waste, Fraud, and Abuse	10

CONTENTS (continued)

Security Areas..... 11

Escorting 11

Vouching 12

Controlled & Prohibited Articles..... 12

Identifying and Protecting Information 12

Unclassified Controlled Information 12

Official Use Only (OUO) 13

Protecting UCI 13

Identifying Classified Matter 14

Classified Matter Levels, Categories, and Access Criteria..... 14

Classification Help 15

Protecting Classified 15

DOE’s Classified Information No Comment Policy 16

Security Incidents 16

Security Incident Management Program (SIMP)..... 16

Common Causes..... 16

Reduce Your Risk..... 17

Counterintelligence Program..... 17

Did You Know..... 17

Who Is a Target? 17

Foreign Intelligence Service Tactics 17

Be Vigilant..... 18

Protect Yourself 18

Comprehensive Security Briefing Quiz/Completion Record 19

SNL's resume highlights:

Radar
Super-computers
Clean rooms
Proximity fuses
Nuclear weapons

Overview and Background

We Are a National Security Laboratory

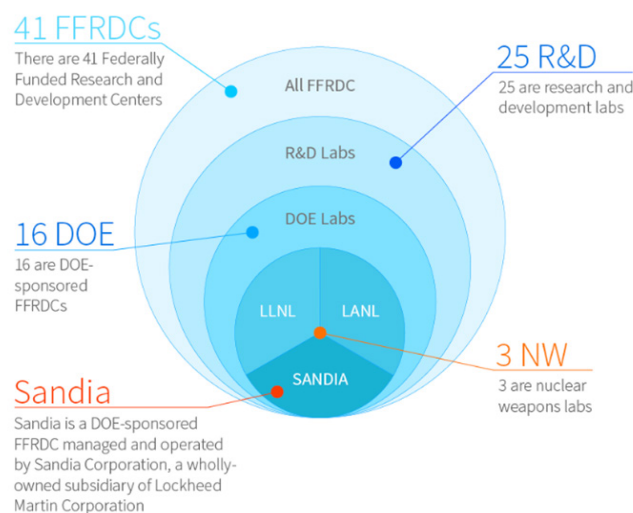
Sandia is one of several DOE National Laboratories, part of the world's most advanced research network dedicated to weapons and energy work.

Our work has been crucial to America's success since 1949.

We are currently pioneering even more technological advances. The work we do here today will have an effect on our future; thus, other countries and companies are very interested in what we are doing.

Where Do You Fit In?

You are part of a large organization that has been entrusted to do very important work for the U.S. government. The American people have entrusted us to protect classified matter, including information about nuclear, chemical, and biological research, and other controlled information.



Security Threats are Real

Threats

- Adversaries
People and governments want the information we have.
 - ◇ Insiders—Clandestine intelligence gathering is a reality. Also, some workers are willing to share information for various reasons (money, recognition, ideology, etc.).
 - ◇ External operatives—Espionage is an ever-present reality, whether conducted by foreign governments or industrial spies.
- Inadvertent disclosure
Information can be compromised due to human error.
 - ◇ Carelessness is as big a threat as spies.
 - ◇ Changes in routine can lead to mistakes.
 - ◇ Failure to recognize vulnerabilities can result in lost information.
 - ◇ Ignoring established controls can create opportunities for adversaries.

Risks

- Harm to national security
- Loss of America's technological and military superiority
- Damage to Sandia's reputation
- Loss of Sandia's contract
- Termination



Some Sobering Facts

Did you know that **New Mexico** is a hot spot for spies? Counterintelligence reports that for many international intelligence operatives, the state's name is nearly synonymous with espionage.

Silicon Valley in California is also a hotbed for espionage. According to the FBI, Silicon Valley is home to many of the estimated 3,000 front companies nationwide that have been set up by foreign countries to steal secrets and acquire technology.

Use Operations Security (OPSEC)

- **Think.** Recognize and acknowledge that you are at risk.
- **Assess.** Evaluate your routines and your environment. Where are you vulnerable?
- **Protect.** Adopt security measures and work controls, and make security a part of everything you do.

You Already Understand and Practice Security

At home, you know the risks and the consequences. We need you to be as diligent at work as you are at home.



*Did you know
that New Mexico
is a hot spot for
spies?*

You leave for work and can't recall if you closed the garage...so you go back and check.

Yet we have situations where people suspected they left a safe open, but went home anyway.



You lock the doors of your car...automatically.

But we have a high number of people leaving their classified network open and unlocked.

You test the front door after you lock it to ensure that it is, indeed, locked.

Yet many safes that were thought to be closed are found open because people didn't test the lock.

You keep your wallet in a safe place.

But we've found passwords taped to the back of monitors and under keyboards.

Seemingly insignificant bits of information can be combined to build a bigger picture.

You must need the information to do your work...a concept known as need to know (NTK).

Information Must Be Protected

This applies to both classified and unclassified. Seemingly insignificant bits of information can be combined to build a bigger picture.

Would you...

Share your address with a stranger?

Give a coworker your credit card number?

Reveal your Social Security Number?

None of this information is classified, but think of the damage that can be done when this information is combined.

Need to Know

Your clearance is your **access authorization**, but it does not give you permission to access all information. You must need the information to do your work, a concept known as need to know (NTK).

You don't have the right to pick something up off of someone else's desk just because you have a clearance. You must have NTK to view any classified or unclassified controlled information (UCI).

Likewise, the people with whom you share information must have NTK. Just because a coworker has a clearance doesn't mean they need access to the information with which you have been entrusted.

Understanding the Clearance Process

Personnel Security Program Purpose

The Department of Energy (DOE) Personnel Security Program establishes requirements that ensure DOE's missions are accomplished in a secure environment by men and women in whom both the DOE and the American people may place their complete trust and confidence. A **security clearance** is an administrative determination that an individual is eligible for access to classified information. An **access authorization** (security clearance) is an administrative determination that an individual is eligible for access to particular types or categories of classified information or material.

No individual will have access to classified information or Special Nuclear Material (SNM) unless that individual has been granted the appropriate security clearance and possesses a NTK. Access to, knowledge of, or possession of classified information or SNM will not be afforded to any individual solely by virtue of the individual's office, position, or security clearance.

Security Clearances

Security clearances denote an individual's eligibility for access to a particular type of classified information or material, such as National Security Information, Restricted Data (RD), Formerly Restricted Data, or Special Nuclear Material. In determining such eligibility, DOE may investigate and consider any matter that relates to the determination of whether access is clearly consistent with the interests of national security. Generally, DOE issues Top Secret, Secret, and Confidential security clearances, and Q and L access authorizations.

Personnel security investigations are conducted for DOE by the Office of Personnel Management (OPM), the Federal Bureau of Investigation (FBI), or other federal agency authorized to conduct background investigations.

Adjudication

Security clearance determinations are based on information acquired through the investigation conducted on the applicant or employee or otherwise available to personnel security officials.

All individuals' initial and continued eligibility for security clearances are adjudged against the Adjudicative Guidelines for Determining Eligibility for Access to Classified Information (Guidelines). Where the Cognizant Personnel Security Office (CPSO) has no information related to any of the areas of concern identified in the Guidelines, either from the report of investigation or from other sources, a favorable determination must be made. Where the CPSO has information related to any areas of concern identified in the Guidelines, either from the report of investigation or from other sources, such information will be regarded as derogatory and create a question as to the individual's security clearance eligibility. If questions as to the individual's security clearance eligibility can be favorably resolved in accordance with the processes and considerations set forth in the Guidelines, the appropriate security clearance must be granted or continued.

An access authorization is an administrative determination that an individual is eligible for access to particular types or categories of classified information or material.

If questions as to the individual's security clearance eligibility can be favorably resolved in accordance with the processes and considerations set forth in the Guidelines, the appropriate security clearance must be granted or continued.

The adjudication process is the careful weighing of a number of variables, known as the whole person concept, utilizing the National Guidelines.

The adjudication process is the careful weighing of a number of variables, known as the whole person concept, utilizing the Guidelines. In evaluating the relevance of an individual's conduct, the CPSO will assess the disqualifying and mitigating conditions outlined in the Guidelines, which take the following factors into account:

- the nature, extent, and seriousness of the conduct
- the circumstances surrounding the conduct, to include knowledgeable participation
- the frequency and recency of the conduct
- the individual's age and maturity at the time of the conduct
- the voluntariness of participation
- the presence or absence of rehabilitation and other permanent behavioral changes
- the motivation for the conduct
- the potential for pressure, coercion, exploitation, or duress
- the likelihood of continuation or recurrence

Due Process

When applicants and employees are determined to not meet the standards for access to classified information, the CPSO initiates the Administrative Review procedures to deny or revoke a security clearance, as set forth in 10 CFR 710. These procedures are established to ensure that an individual is afforded full due process in a manner consistent with traditional American concepts of justice and fairness.

These procedures are established to ensure that an individual is afforded full due process in a manner consistent with traditional American concepts of justice and fairness.

References: Executive Order 12968, Access to Classified Information (dated 8-7-95); *Adjudicative Guidelines for Determining Eligibility for Access to Classified information* (Adjudicative Guidelines (dated 12-29-04); Title 10, Code of Federal Regulations, part 710 (10 CFR 710), *Criteria and procedures for Determining Eligibility for Access to Classified Material or Special Nuclear Material*; DOE Order 472.2, *Personnel Security* (dated 7-21-11); DOE O 475.1, *Counterintelligence Program* (dated 12-10-04)

About That Badge

Think of your badge as your key. You use your key to get into your house or your car. At SNL, your badge is the key you use to get into work. You need to protect your badge like you protect your house or car keys.

SNL Local Site-specific Only (LSSO) Badges

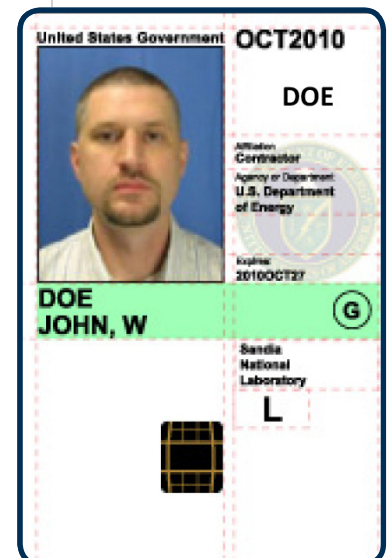
LSSO badges are used only at specific sites. At SNL, they are required if you don't have an HSPD-12 credential.



If you don't recognize the person or the badge, play it safe and don't let him in.

Homeland Security Presidential Directive 12 (HSPD-12)

HSPD-12 established a federal credential, which is now the most common form of identification at SNL. However, unlike DOE-issued credentials, other federal agencies don't specify clearance levels on the credentials they issue. If you don't recognize the person or the badge, play it safe and don't let them in.



Unauthorized disclosure -
The transfer, via any means, of classified or sensitive information or material to someone who is not authorized to receive such information.

Standard Form (SF) 312, *Classified Information Nondisclosure Agreement*

- Contract between you and the U.S. Government.
- You agree to protect classified information from *unauthorized disclosure*.
- You are required to sign the SF312 at an SNL Badge Office or SNL remote site.

Badge Responsibilities

With your badge come certain responsibilities.

• Do

◊ Wear it:

- Above your waist
- Over any outerwear

◊ Renew if:

- It becomes faded or damaged
- Your physical appearance significantly changes
- Your name changes

◊ Report to badge office immediately if:

- Lost
- Stolen

◊ Return if:

- You take an extended leave of absence (90 consecutive calendar days or longer)
- Your clearance is no longer required
- Your clearance level changes
- You separate from SNL
- Your HSPD 12 badge expires
- You receive an HSPD 12 badge to replace your LSSO badge

You'd want your house key back if your house sitter no longer needed access to your home.

• Don't:

- ◊ Wear your badge offsite
- ◊ Use it for personal identification
- ◊ Allow it to be photocopied



CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT	
AN AGREEMENT BETWEEN	AND THE UNITED STATES
(Name of Individual - Printed or Typed)	
<p>1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12958, or under any other Executive Order or statute that prohibits the unauthorized disclosure of information in the interest of national security, and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in Sections 1.1, 1.2, 1.3 and 1.4 of Executive Order 12958, or under any other Executive Order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.</p> <p>2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.</p> <p>3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of the information or last granting me a security clearance that such disclosure is permitted; I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.</p> <p>4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or the termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal law, including the provisions of Sections 641, 793, 794, 796, 792, and 1824, Title 18, "the provisions of Section 783(b), Title 50, United States Code, and the provisions of the Intelligence Identities Protection Act of 1949. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.</p> <p>5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation of classified information not consistent with the terms of this Agreement.</p> <p>6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.</p> <p>7. I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of Sections 793 and/or 1824, Title 18, United States Code, a United States criminal law.</p> <p>8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.</p> <p>9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.</p> <p>(Continue on reverse.)</p>	

Maintaining Your Clearance

Your badge provides evidence of your identity and can be thought of as your key to SNL. It's important to know that:

- Being granted a clearance does not guarantee you will remain cleared or retain employment forever.
- You can lose your clearance and may be terminated for:
 - Theft of government property.
 - Careless handling of, failure to protect, or disclosure of classified matter.
 - Habitual use of alcohol without rehabilitation or reformation.
 - Use of illegal drugs, or legal drugs without a prescription.
 - Gross misconduct.
- Anything the U.S. government believes could call into question your trustworthiness or integrity should be reported.
- Corporate Investigators know that mistakes happen, and bad things happen to good people.
 - Don't give them a reason to question you.
 - Don't try to hide anything—it will come out during an investigation.

You can't be coerced or blackmailed if you don't have anything to hide.

Certain prescribed drugs, such as medicinal marijuana, are not allowed on federal property (DOE, SNL, etc.).

Report Waste, Fraud, and Abuse

You must report to Corporate Investigations if you suspect that someone is committing waste, fraud, or abuse.

Examples

Waste: Ordering 10 replacement parts for a piece of equipment that will never be used, just to spend year-end funds.

Fraud: Submitting an expense report that contains false information.

Abuse: Using a Sandia computer, printer, or telephone for outside employment.

Fraud: Coming to work late, taking long lunches, and leaving early, but recording full shifts on your time sheet.

Abuse: Using a government vehicle to deliver Avon products around the Labs.

The important thing is to not engage in such activities and to report anyone who does.

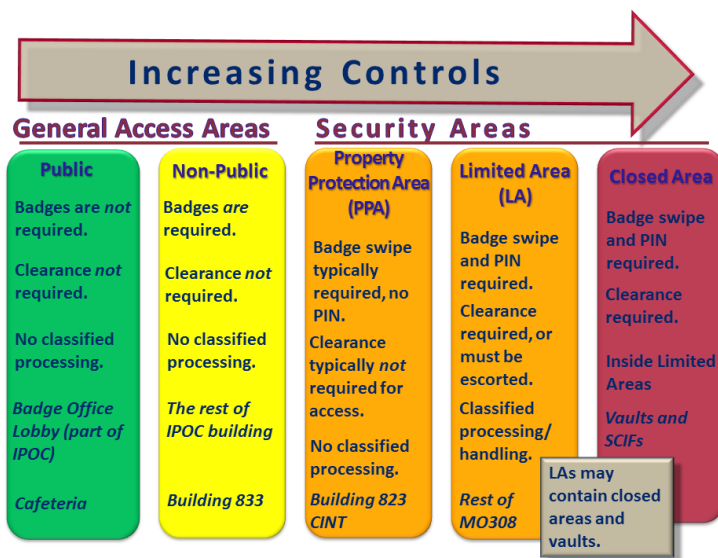


Additional security-related reporting requirements are addressed in the DOE and Sandia Reporting Requirements pamphlet, which is attached to this booklet. The pamphlet can also be found online or by contacting Corporate Investigations.

Security Areas

Each security area has different requirements for what you can or cannot bring in.

Sandia-controlled premises contain many different types of security areas. You may also hear the phrase “technical area” or “tech area.” This describes certain geographic boundaries. Tech areas may contain various types of security areas.



Escorting

Escorting is required in limited or more restricted areas where classified work is done.

- **To be an escort, you must:**
 - ◊ Have appropriate access authorization (Q or L clearance).
 - ◊ Possess a DOE-approved badge.
 - ◊ Be a U.S. citizen.
- **When escorting uncleared individuals, you must:**
 - ◊ Take measures in advance to prevent compromise of sensitive information, especially classified.
 - ◊ Escort no more than eight uncleared individuals at a time.
 - ◊ Observe all requirements of spaces visited.
 - ◊ Explain safety and security requirements for the area being visited.
 - ◊ Upon transfer of escorting duty, ensure that the new escort accepts responsibility.

- **Escorting Foreign Nationals:**

Special rules apply to both cleared and uncleared Foreign Nationals, especially regarding areas they may visit. See your manager or Security Coordinator for guidance.

- ◊ Foreign Nationals (cleared and uncleared) must have an approved Foreign National Request (FNR) Security Plan (SP).
- ◊ Foreign Nationals (cleared and uncleared) are allowed only in areas listed on the FNR SP.
- ◊ Hosts and escorts must be listed on the FNR SP.

Note: SNL/CA has additional, site-specific escorting requirements. Members of the Workforce at that site should contact Security Awareness or Visitor Control to ensure they are aware of their responsibilities.



Vouching

If you use your badge to allow another individual access to SNL, you accept responsibility for that individual. At a minimum, check the badge for appropriate government agency (DOE), expiration date, and proper clearance level for the area and verify that no unauthorized controlled articles or prohibited articles are being brought in. Ultimately you are responsible for any consequences associated with allowing unescorted access.

Controlled and Prohibited Articles

Each security area has different requirements for what you can or cannot bring in.

- Controlled articles are “gadgets” that can record, store, or transmit data and are capable of compromising information. All L- and Q-cleared members of the workforce who wish to bring their non-government owned Portable Electronic Devices (PEDs) into Sandia’s Limited Areas must read and acknowledge the Rules of Use (PEDS100). The Rules of Use specifically address the PED user’s responsibilities as well as the consequences of unallowable use of a PED.

Note: Even if you choose not to bring your non-government owned PED(s) into the Limited Areas, you are encouraged to read the Rules of Use.

- Prohibited articles are things that can harm you or property, or are illegal. Although certain programs at SNL are approved to work with prohibited articles, personally-owned articles are not allowed anywhere on Sandia-controlled premises.

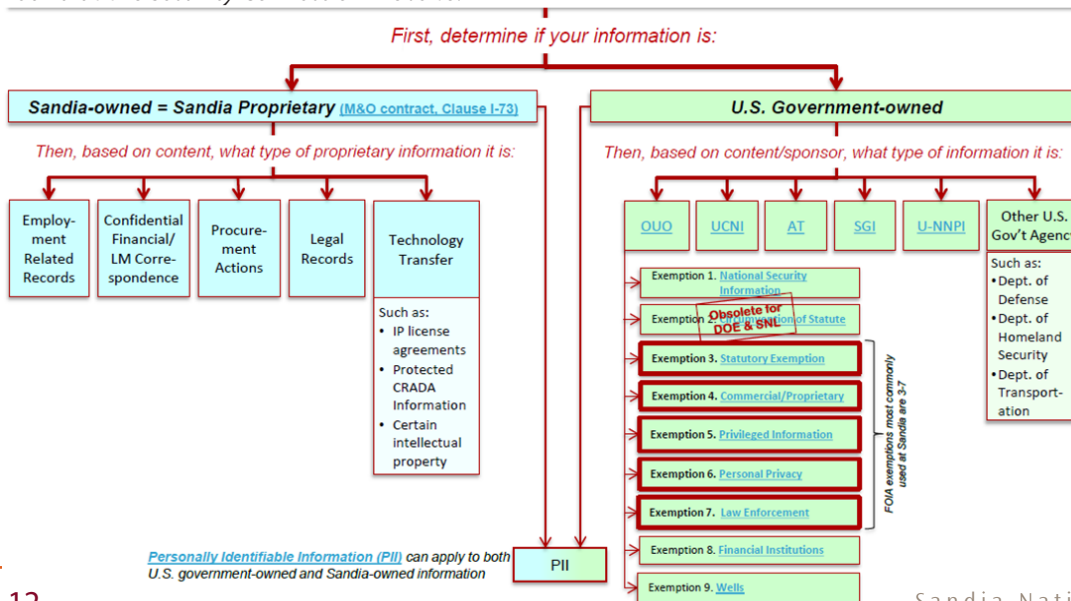
Examples	
Controlled Articles	Prohibited Articles
Recording equipment	Explosives
Cell phones	Dangerous weapons
iPods/iPads	Alcohol
Cameras	Controlled Substances*
USB Devices	

*For prescription drugs, you must be able to produce a doctor’s prescription under your name. Certain prescribed drugs, such as medicinal marijuana, are not allowed on federal property (DOE, SNL, etc.) even in states where they are otherwise legal.

Identifying and Protecting Information

Unclassified Controlled Information

There are several different types of Unclassified Controlled Information (UCI), as illustrated below. For each type of UCI, there are different marking and handling requirements. You are responsible for determining the type of information based on the chart below. More information can be found at the *Security Connection* website.



Unclassified Controlled Information (UCI)

– Information for which disclosure, loss, misuse, alteration, or destruction could adversely affect national security, Sandia National Laboratories, or our business partners. Identification and protection of this type of information is required by the code of federal regulations, public law, governmental directives, DOE Orders, contracts with business partners, or Sandia’s processes to protect commercially valuable information.

Official Use Only (OUO)

OUO is the most common type of UCI. If it could damage government, commercial, or private interests if released, and it falls under one of the Freedom of Information Act (FOIA) exemptions, then it's OUO. Always evaluate information:

- At the original draft stage
- After each revision
- Before distributing
- Before disposing

FOIA Exemption	Category Name	What it Protects
Exemption 1	Classified	Never used for OUO. It is only used for classified information.
Exemption 2	Circumvention of Statute	OBSOLETE for DOE & SNL
Exemption 3	Statutory Exemption	Information whose disclosure is specifically protected by law and not otherwise controlled
Exemption 4	Commercial/Proprietary	Trade secrets, commercial or financial information, if released could impair the government's ability to obtain information in the future
Exemption 5	Privileged Information	Interagency or intra-agency memos or letters not available by law to a party unless the party is in litigation with the agency
Exemption 6	Personal Privacy	Information that could cause an individual personal distress or embarrassment, or expose them to identity theft
Exemption 7	Law Enforcement	Information that if released could endanger the life or physical safety or disclose techniques and procedures for law enforcement investigations or prosecutions.
Exemption 8	Financial Institutions	Evaluation of a financial institution's stability
Exemption 9	Wells	Geological and geophysical information and data, resource maps, and new drilling techniques

Protecting UCI

A security clearance is not required for UCI access. In general, information may be given to a person who needs it to perform his/her duties. Some UCI (e.g., Export Controlled Information) has additional access restrictions.

Property Protection Area

Keep UCI in one of the following:

- Individual, locked office
- Locked suites or offices
- Locked receptacle

Limited Area

- UCI documents may be left on a desktop in a Limited Area as long as the materials have been turned over to a blank sheet.
- Personally Identifiable Information (PII) and Unclassified Controlled Nuclear Information (UCNI) should be stored in a locked office or receptacle.

Marking

- Proper marking of UCI documents/matter will help you properly store and protect them.
- Proper marking of UCI email messages will stop them from going outside the firewall (Outlook Email Marking Assistant).
- Proper marking of UCI faxes will alert the recipient to protect the information.

Computers

Protect UCI on shared servers/computers to prevent access by persons without NTK.

Distribution

Sandia has an online Review & Approval tool to help review and mark UCI intended for distribution and prevent the unintentional release of classified or sensitive information.

Before submitting an item for review consider the sensitivity level of the information and the NTK of the receiving audience.

Communication

- Do not use wireless handset telephones or cell phones for sensitive conversations.
- Use secure telephone equipment (STE) phones whenever possible.
- Close office or conference room doors.
- Do not discuss UCI in public areas such as break rooms, hallways, restaurants, or airports/airplane.

Identifying Classified Matter

Classified **matter** is any combination of documents and material containing classified information. Classified **information** is information that is classified by statute or executive order. Access is restricted to persons with an access authorization (security clearance) and a “need-to-know.” Classified matter is *compartmented* to ensure that no one has more information than he/she needs. If you work with classified, you will only see a limited amount of what is out there.

Classified comes in many forms: it could be a paper document, a computer disk, or a piece of hardware. It could also be a thumb drive that contains classified information, an e-mail, or a laboratory notebook. You could even have a classified conversation.

Classified Matter Levels, Categories, and Access Criteria

Categories specify the type of classified matter.

Levels indicate the sensitivity of classified matter.

Damage is based on the level of sensitivity and indicates possible consequences to national security.

As risk increases, so do protection measures, including clearance level for access.

Classification Level	Classification Categories and Clearance Levels			Degree of Damage (if released)	Increasing Risk
	Restricted Data (RD)	Formerly Restricted Data (FRD)	National Security Information (NSI)		
Top Secret (TS)	Q only	Q only	Q only	Exceptionally Grave	
Secret (S)	Q only	Q and L	Q and L	Serious	
Confidential (C)	Q and L	Q and L	Q and L	Undue	



Special Nuclear Material –
Special Nuclear Material (SNM) is fissionable material that is especially useful in nuclear weapons. SNM is protected according to its attractiveness and the ease with which it can be turned into a weapon.

If you work with SNM you will receive specific training beforehand.

Always protect information at the highest level and category until you get a DC review.

Classification Help

- **Derivative Classifier (DC)** An individual authorized to confirm that an unmarked document or material is unclassified or determine that it is classified as allowed by his or her description of authority.
 - Only trained DCs determine whether documents and material are classified, and to what level and category.
 - DCs are trained on specific technologies/programs.
 - What is not classified on one technology may be classified in other circumstances. Make sure you choose the right DC.
 - You can find a DC in your subject area at the Sandia “Security” website or by calling 321 from a Sandia phone or 845-1321.
- **Classified Administrative Specialists (CASS)** Individuals trained to mark, store, duplicate, destroy, and mail classified matter.
- **Classification Office:** You can always challenge a DC determination if you think the determination is incorrect. Contact the *Classification Office* (505 844-5574) for more information.
- **Derivative Declassifiers (DDs)** An individual authorized to declassify or downgrade documents or material that an employee believes no longer requires protection, in specified areas as allowed by his or her description of authority and are located in the Classification Office.
- **DOE Office of Classification:**
 - If the challenge cannot be resolved locally, the employee has the right to submit a challenge in writing to the Director, Office of Classification.
 - Every employee has the right at any time to submit a challenge in writing directly to the Director, Office of Classification. Under no circumstances is the employee subject to retribution for making a challenge.

Protecting Classified

Classified matter must be protected. The higher the risk, the higher the classification. Therefore, all classified matter must be protected to the **highest level and category** until you get a DC review.

You must get a review in the following situations:

- *In Limited Area or more restricted areas.*
- *Using computers on the Sandia Classified Network (SCN) or on an approved stand-alone system.*
- *Using secure forms of telecommunication and other electronic transmissions.*

- A newly generated document or material in a classified subject area that potentially contains classified information
- An existing, unmarked document or material that an employee believes may contain classified information
- An existing, marked document or material that an employee believes may contain information classified at a higher level or more restrictive category
- A document or material generated in a classified subject area and intended for public release (e.g., for a publicly available webpage, for news organizations), including documents provided to or testimony given to Congress
- Extracts. A newly generated document that consists of a complete section (e.g., chapter, attachment, appendix)

DOE's Classified Information No Comment Policy

If asked about classified information:

- State only, "We don't comment on items in the public domain."
- **Do not** comment on the classification status or technical accuracy of the information.
- **Do not** confirm or deny.

Acknowledgement can be an **indicator** to an adversary. Refer questions to Media Relations.

- This applies to commenting on news strings, Facebook, etc.

Report DOE classified information in open source, in person, to the Classification office (505-844-5574).

Consequences of failing to meet your responsibilities regarding classified can include termination and/or civil and criminal penalties.

Security Incidents

Security Incident Management Program (SIMP)

SIMP conducts inquiries into potential security incidents. The Inquiry Officials collect facts, mitigate the incident, and work with organizations to prevent recurrence.

If you suspect you have caused an incident or witnessed one, you must report to SIMP. An inquiry will determine whether an incident has actually occurred. SIMP Inquiry Officers are on call 24 hours a day, 365 days a year. The pager number for after-hours reporting is (505) 283-7467. Report as soon as you can!

An **incident** is a potential compromise of information or noncompliance with DOE directives or corporate policy.

- Must be investigated.
- May be a violation of federal law.

An **inquiry** is a review of the circumstances to develop all pertinent information and to determine whether an infraction, or a compromise, or potential compromise has occurred.

An **infraction** is documentation of administrative and/or disciplinary actions assigned to an individual taken in response to an incident of security concern.

Common Causes

Security incidents are mostly caused by:

- Being careless, making assumptions, or becoming overconfident.
- Distractions and interruptions.
- Changes in routine.
- Time pressures.
- Misperception of risk.

Recognize when you are at risk and pause, step back, and regroup. Be aware that you can cause distractions. Don't interrupt others while they're performing tasks that have the potential for error, such as securing a closed area or safe, or even something as simple as entering a Limited Area.

Sandia has a similar no comment policy. Refer questions to Media Relations.

Unauthorized disclosure:

The transfer, via any means, of classified or sensitive information or material to someone who is not authorized to receive such information.

When an incident occurs

- *Report immediately or have someone report on your behalf.*
- *Don't discuss details over the phone.*
- *"Incidents" don't always result in "infractions."*



Over 80% of information collected about SNL is from open sources. You can learn a lot from information that has been posted on the web.

Reduce Your Risk

- Create a routine. Perform a self-check prior to entering Limited Areas to make sure you don't have unauthorized controlled articles with you.
- Talk to your family about Sandia's security rules so they don't inadvertently cause you to have an incident. An example of how this can happen: Your spouse tries to surprise you with a new electronic gadget as a birthday present, putting it into your briefcase so that you'll find it when you get to work.

Counterintelligence Program

The Counterintelligence Program is designed to counter the efforts of enemy spies, counter threats posted by terrorists/homegrown violent extremists, investigate and maintain U.S. Intelligence Community liaison, and protect you.

Did You Know

- One third of people passing information have no clearance. This means that people who didn't have access to classified still found valuable information to share, such as travel itineraries, fields of research, etc.
- More than twice as many people volunteer to be a spy than are recruited. People want money, recognition, and fame.
- Today's agents are professors, engineers, and businessmen. They're criminal capitalists who see only dollar signs.
- Spies don't just work for governments; some work for private enterprise. They are not spies like you see in the movies. These are regular folks. You cannot determine who's a threat based on nationality, appearance, etc.
- Two-thirds of adversaries used social media to establish contact with an insider. Be careful of what you put out there, and be careful talking to strangers. Be aware that other people may be posting information about YOU! Cancelling your accounts doesn't make the information go away.

Who is a target?

Potential targets of foreign intelligence services are:

- People with a clearance.
- People who have access to someone with a clearance.
- Any type of media that might contain useful information.

Foreign Intelligence Service Tactics

- Hacking electronic media (e.g., computers, social networks).
- Eliciting during conferences/trade fairs.
- Tasking foreign students at U.S. universities.
- Sexspionage.
- Debriefing foreign visitors to the U.S. routinely.
- Targeting ethnic employees/scientists.
- Use of interpreters.

Be Vigilant

- Increased use of computers makes us vulnerable. Hackers and cyber criminals target our electronic media for information or other actions, such as a denial of service attack. Be careful: the internet provides a sense of anonymity and a false sense of security.
- All foreign travel to sensitive countries requires a Counterintelligence briefing.

Protect Yourself

- Don't place sensitive information on social networks.
- Don't provide unnecessary details about you or your work in social interactions; adversaries can compile information about you from different sources, which puts you at risk.
- Maintain a skeptical attitude; be aware when things don't seem right.
- Plan ahead—know what you're going to say if someone asks you about your work.



If you suspect you've been targeted or see suspicious activity, contact the Counterintelligence Office.

New Mexico - (505) 284-3878

California - (925) 294-6616

CI Helpline - CIhelp@sandia.gov

You may not realize you've been targeted.

There are special reporting requirements associated with foreign interactions.

Security & **YOU**
Think.
Assess.
Protect.

Comprehensive Security Briefing Quiz/Completion Record

You must correctly answer the following questions:

1. "Access authorization" is another term for _____.
2. Your clearance alone does not permit you to access classified matter; you must also have which of the following:
 - ☐ Derivative classifier's permission
 - ☐ Need to Know
 - ☐ *a* and *b*
 - ☐ All of these
3. Which of the following are possible consequences (aka: risks) of poor security? Check **all** that apply.
 - ☐ Harm to national security
 - ☐ Loss of America's technological and military superiority
 - ☐ Damage to Sandia's reputation
 - ☐ Loss of Sandia's contracts
 - ☐ Termination (of responsible individuals)
 - ☐ Fines and/or imprisonment
4. The concept of OPSEC can be effectively summarized in these three words: _____, _____, _____.

Hint: These terms can be defined as follows:

 - Recognize and acknowledge that you are at risk.
 - Evaluate your routines and your environment.
 - Adopt security measures and work controls.
5. Uncleared foreign national visitor badges are this color: _____.
6. Which of the following are you **not** allowed to do with your badge? Check **all** that apply.
 - ☐ Use it for personal identification
 - ☐ Use it to vouch others into Limited Areas
 - ☐ Wear it offsite
 - ☐ Allow it to be photocopied
 - ☐ Wear it in General Access Areas
7. If your badge is lost or stolen, what immediate action must you take? _____
8. **True** or **False**: Medicinal marijuana is allowed on Sandia-controlled premises in states where possession has been legalized.

Hint: Your clearance is granted by the federal government and SNL is considered DOE property.
9. Classified processing is allowed in which of the following areas? Check **all** that apply.
 - ☐ General Access Area (GAA)
 - ☐ Property Protection Area (PPA)
 - ☐ Limited Area (LA)
 - ☐ Closed Area (CA)

10. Escorts must (check **all** that apply):

- ☐ Be a Sandia employee
- ☐ Have appropriate clearance
- ☐ Possess a DOE-approved badge
- ☐ Be a U.S. citizen

11. If you choose to vouch another cleared individual into a Limited Area, you must do which of the following at a minimum? Check all that apply.

- ☐ Escort the person to their actual destination
- ☐ Perform a badge check (expiration date, agency, clearance level)
- ☐ Verify that the person has no prohibited or controlled articles
- ☐ Instruct the individual to notify the Facility Manager of his/her presence in the area
- ☐ All of these

12. **True** or **False**: All information at SNL must be protected, even unclassified information.

13. You should evaluate UCI at which stage(s) to determine whether it is OUO? Check **all** that apply.

- ☐ At original draft stage
- ☐ After each revision
- ☐ Before distributing
- ☐ Before disposing

14. Classified information may be processed only on which type(s) of computer?

- ☐ Internal Restricted Network (IRN)
- ☐ Sandia Classified Network (SCN)
- ☐ Approved stand-alone systems
- ☐ *a* and *b*
- ☐ *b* and *c*
- ☐ Any of these

15. When marking classified documents, which **one** element **does not** need to be included?

- ☐ Highest level and category
- ☐ Markings on top and bottom of each page
- ☐ Anticipated expiration date
- ☐ Markings on front and back
- ☐ Cover and backing sheets

16. Which of the following individuals determines whether documents or material are classified, and to what level and category?

- ☐ Classified Administrative Specialist (CAS)
- ☐ Safeguards and Security (S&S) Coordinator
- ☐ Security Awareness Coordinator
- ☐ Derivative Classifier (DC)

17. Acknowledgement can be an _____ to an adversary.

18. What are some common causes of security incidents?

- ☐ Being careless
- ☐ Distractions
- ☐ Changes in routine
- ☐ All of the above

19. Potential targets of foreign intelligence services include:

- ☐ People with a clearance
- ☐ People who have access to someone with a clearance
- ☐ Any type of media that might contain useful information
- ☐ All of these

20. **True** or **False**: You are a target of espionage.

SEC150 COMPLETION RECORD

Print Full Name (Last, First, Middle): _____

SNL Org # or Company Name: _____

☐ Employee ☐ Contractor ☐ Consultant ☐ Student ☐ KMP

After reading all the modules of SEC150:

1) Please enter the authorization code provided by your company's Facility Security Officer or other authorized individual:

2) Sign below confirming you have read and understand the briefing.

I have read and understand all the modules in SEC150, *Comprehensive Security Briefing*, and understand that I cannot access classified matter or Special Nuclear Material (SNM) at any site until I have turned in a completed SF-312, *Classified Information Non-disclosure Agreement*, to an SNL Badge Office.

Signature: _____

Date: _____

3) Send the completed quiz and signed completion record via e-mail to securityed@sandia.gov or via fax to 505-844-7802.
You must score an 85 percent or higher to receive credit for this briefing.

4) If you would like confirmation of receipt, provide your e-mail or fax number (please write legibly).



Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under Contract DE-AC04-94AL85000.
SAND2015-8170 TR. Approved for public release; further dissemination unlimited.

DOE and Sandia Reporting Requirements

What You Need to Know About Your Reporting Responsibilities



Revised: October 15, 2015

"Employees are encouraged and expected to report any information that raises doubts as to whether another employee's continued eligibility for access to classified information is clearly consistent with the national security."

—Executive Order 12968, *Access to Classified Information*

Concerns of Personnel Security Interest

If you			Report to	By this date
General Rmpts	Are approached or contacted by ANY individual seeking unauthorized access to classified matter or special nuclear material (SNM).		NM—Counterintelligence (505-284-3878) or SIMP pager (505-283-7467) CA—Counterintelligence (925-294-1362), Security (925-294-2300), or SIMP (321 or 925-294-2600)	Immediately.
	Are aware of information about other Members of the Workforce that raises concerns of personnel security interest. Note: Such information must be reliable and relevant, and create a question as to the individual's access authorization eligibility.		NM—Corporate Investigations (505-845-9900) CA—Clearance Processing (925-294-2061)	Immediately.
Legal Issues	*Are arrested; subject to criminal charges (including charges that are dismissed); receive citations, tickets, or summonses; or are detained by federal, state, or other law-enforcement authorities for violations of the law within or outside of the U.S.		NM—Corporate Investigations (505-845-9900) CA—Clearance Processing (925-294-2061)	Orally within 2 work days of occurrence, and in writing within the next 3 work days.
	Note: Traffic citations/tickets/fines are reportable only if they exceed \$300 and only when the fine is assessed, unless drugs or alcohol were involved. (Assessed means you agree to pay or you go to court and the court's ruling equals a fine above \$300. Court fees or other administrative costs associated with the traffic citation/ticket/fine should not be added to the final assessed amount.)		NM—Corporate Investigations (505-845-9900) CA—Clearance Processing (925-294-2061)	Orally within 2 work days of occurrence, and in writing within the next 3 work days.
Citizen-ship	*File for bankruptcy, regardless of whether it is for personal or business-related reasons.		NM—Corporate Investigations (505-845-9900) CA—Clearance Processing (925-294-2061)	Orally within 2 work days of occurrence, and in writing within the next 3 work days.
	*Have your wages garnished for ANY reason. Examples: divorce, debts, child support.		NM—Corporate Investigations (505-845-9900) CA—Clearance Processing (925-294-2061)	Orally within 2 work days of occurrence, and in writing within the next 3 work days.
Life Circumstances	*Change citizenship or acquire dual citizenship.		NM—Corporate Investigations (505-845-9900) CA—Clearance Processing (925-294-2061)	Orally within 2 work days of occurrence, and in writing within the next 3 work days.
	*Are a foreign citizen who changes citizenship.		NM—Corporate Investigations (505-845-9900) CA—Clearance Processing (925-294-2061)	Orally within 2 work days of occurrence, and in writing within the next 3 work days.
Foreign Travel	*Have legal action resulting in a name change.		NM—Corporate Investigations (505-845-9900) CA—Clearance Processing (925-294-2061)	Orally within 2 work days of occurrence, and in writing within the next 3 work days.
	Marry or cohabitate with a person.		NM—Corporate Investigations (505-845-9900) CA—Clearance Processing (925-294-2061)	Orally within 2 work days of occurrence, and in writing within the next 3 work days.
Foreign Interaction	Note: A cohabitant is a person who lives with the individual in a spouse-like relationship or with a similar bond of affection or obligation, but is not the individual's legal spouse, child, or other relative (in-laws, mother, father, brother, sister, etc.).		NM—Corporate Investigations (505-845-9900) CA—Clearance Processing (925-294-2061)	Orally within 2 work days of occurrence, and in writing within the next 3 work days.
	*Are hospitalized for mental health reasons.		NM—Corporate Investigations (505-845-9900) CA—Clearance Processing (925-294-2061)	Orally within 2 work days of occurrence, and in writing within the next 3 work days.
Foreign Interaction	*Are treated for drug or alcohol abuse.		NM—Corporate Investigations (505-845-9900) CA—Clearance Processing (925-294-2061)	Orally within 2 work days of occurrence, and in writing within the next 3 work days.
	*Use an illegal drug or a legal drug in a manner that deviates from approved medical direction.		NM—Corporate Investigations (505-845-9900) CA—Clearance Processing (925-294-2061)	Orally within 2 work days of occurrence, and in writing within the next 3 work days.
Foreign Interaction	No longer require your clearance, terminate your employment, are on extended leave of 90 calendar days or more, or your access authorization is no longer required for 90 calendar days or more.		NM—Corporate Investigations (505-845-9900) CA—Clearance Processing (925-294-2061)	Orally within 2 work days of occurrence, and in writing within the next 3 work days.
	Have business-related travel to a sensitive or non-sensitive country.		NM—Corporate Investigations (505-845-9900) CA—Clearance Processing (925-294-2061)	Orally within 2 work days of occurrence, and in writing within the next 3 work days.
Foreign Interaction	Have personal foreign travel to sensitive country.		NM—Corporate Investigations (505-845-9900) CA—Clearance Processing (925-294-2061)	Orally within 2 work days of occurrence, and in writing within the next 3 work days.
	Note: While not required to report travel to a non-sensitive country, you should keep a personal record of personal foreign travel for future clearance (re)investigations.		NM—Corporate Investigations (505-845-9900) CA—Clearance Processing (925-294-2061)	Orally within 2 work days of occurrence, and in writing within the next 3 work days.
Foreign Interaction	Related Sandia Rmpts		NM—Corporate Investigations (505-845-9900) CA—Clearance Processing (925-294-2061)	Orally within 2 work days of occurrence, and in writing within the next 3 work days.
	Hold a Special Access Program (SAP) clearance and: • Travel for personal reasons to a sensitive foreign country, or • Travel for business to any foreign country, sensitive or non-sensitive.		NM—Corporate Investigations (505-845-9900) CA—Clearance Processing (925-294-2061)	Orally within 2 work days of occurrence, and in writing within the next 3 work days.
Foreign Interaction	Hold a Sensitive Compartmented Information (SCI) clearance and travel to any foreign country (sensitive or non-sensitive) for personal or business reasons.		NM—Corporate Investigations (505-845-9900) CA—Clearance Processing (925-294-2061)	Orally within 2 work days of occurrence, and in writing within the next 3 work days.
	Have substantive contact with any foreign national.		NM—Corporate Investigations (505-845-9900) CA—Clearance Processing (925-294-2061)	Orally within 2 work days of occurrence, and in writing within the next 3 work days.
Foreign Interaction	Note: "Substantive contact" refers to a personal or professional relationship that is enduring and involves substantial sharing of personal information and/or the sharing of SNL business information.		NM—Corporate Investigations (505-845-9900) CA—Clearance Processing (925-294-2061)	Orally within 2 work days of occurrence, and in writing within the next 3 work days.
	*Are employed by, represent, or have other business-related associations with a foreign or foreign-owned interest, or with a non-U.S. citizen or other individual who is both a U.S. citizen and a citizen of a foreign country.		NM—Corporate Investigations (505-845-9900) CA—Clearance Processing (925-294-2061)	Orally within 2 work days of occurrence, and in writing within the next 3 work days.
Foreign Interaction	*Have an immediate family member who assumes residence in a sensitive country, and when that living situation changes; e.g., your family member returns to the U.S. or moves to another country, sensitive or non-sensitive. (See list of sensitive countries at the International Travel Office website.)		NM—Corporate Investigations (505-845-9900) CA—Clearance Processing (925-294-2061)	Orally within 2 work days of occurrence, and in writing within the next 3 work days.
	* You are required to report these items to the Sandia organizations listed, but you have the option of also reporting them directly to DOE Personnel Security.		NM—Corporate Investigations (505-845-9900) CA—Clearance Processing (925-294-2061)	Orally within 2 work days of occurrence, and in writing within the next 3 work days.

Other Reporting Requirements

Incidents of Security Concern (aka Security Incidents)	Report immediately, but do not provide details over the phone. NM: OOPS (311) <u>and</u> SIMP (505-283-7467) CA: Security Connection (321) or SIMP (925-294-2600); TTR: Central Alarm Station (702-295-8285) Note: Contractors have added responsibility of reporting incidents to their Facility Security Officer (FSO).
°Waste, Fraud, & Abuse	Incidents of waste, fraud, abuse and criminal matters must be reported to Corporate Investigations (505-845-9900) and other appropriate authorities (e.g., manager, security officials).
°Theft of Property	Any theft of Sandia or U.S. Government property must be reported immediately to Corporate Investigations (505-845-9900). Note: All property that is considered stolen, lost, or missing must be reported regardless of value and regardless of whether it is considered controlled or uncontrolled property.
°Wrongdoing	Report incidents of wrongdoing to SNL Corporate Investigations at SNL/NM (505-845-9900). Note: <ul style="list-style-type: none"> • <i>Incidents of wrongdoing</i> are not limited to circumstances listed in the previous table. • You may also report directly to the Office of the Inspector General any information concerning wrongdoing by DOE employees, contractors, subcontractors, consultants, grantees, other recipients of DOE financial assistance, or their employees.
°Drug Use	Report incidents of illegal drugs in the workplace to Corporate Investigations (NM 505-845-9900). This includes, but is not limited to, trafficking in, selling, transferring, possessing, or using illegal drugs. Note: <ul style="list-style-type: none"> • Illegal drugs are prohibited on both Sandia-controlled premises and Kirtland Air Force Base property. • The use of illegal drugs—or legal drugs in a manner that deviates from medical direction—is a serious offense and could result in termination of your clearance and your employment, as well as arrest.

°SNL/CA staff should also call the Security Operations Office (925-294-2975).

Managers' Reporting Requirements

Managers are responsible for immediately reporting to Personnel Security (NM: 505-844-4493, CA: 925-294-1358) when an employee's clearance is no longer required, employment is terminated, individual is on extended leave of 90 calendar days or more, or access authorization is not required for 90 calendar days or more. Ensure completed DOE F 5631.29, *Security Termination Statement*, and badges are immediately delivered to the Clearance Office.

TTR & REMOTE SITES REPORT TO SNL/NM UNLESS OTHERWISE INDICATED.



Sandia National Laboratories

SAND2009-0424P



Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

SEC150

Comprehensive Security Briefing



Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND 2015-8170 TR.